FIG. 1

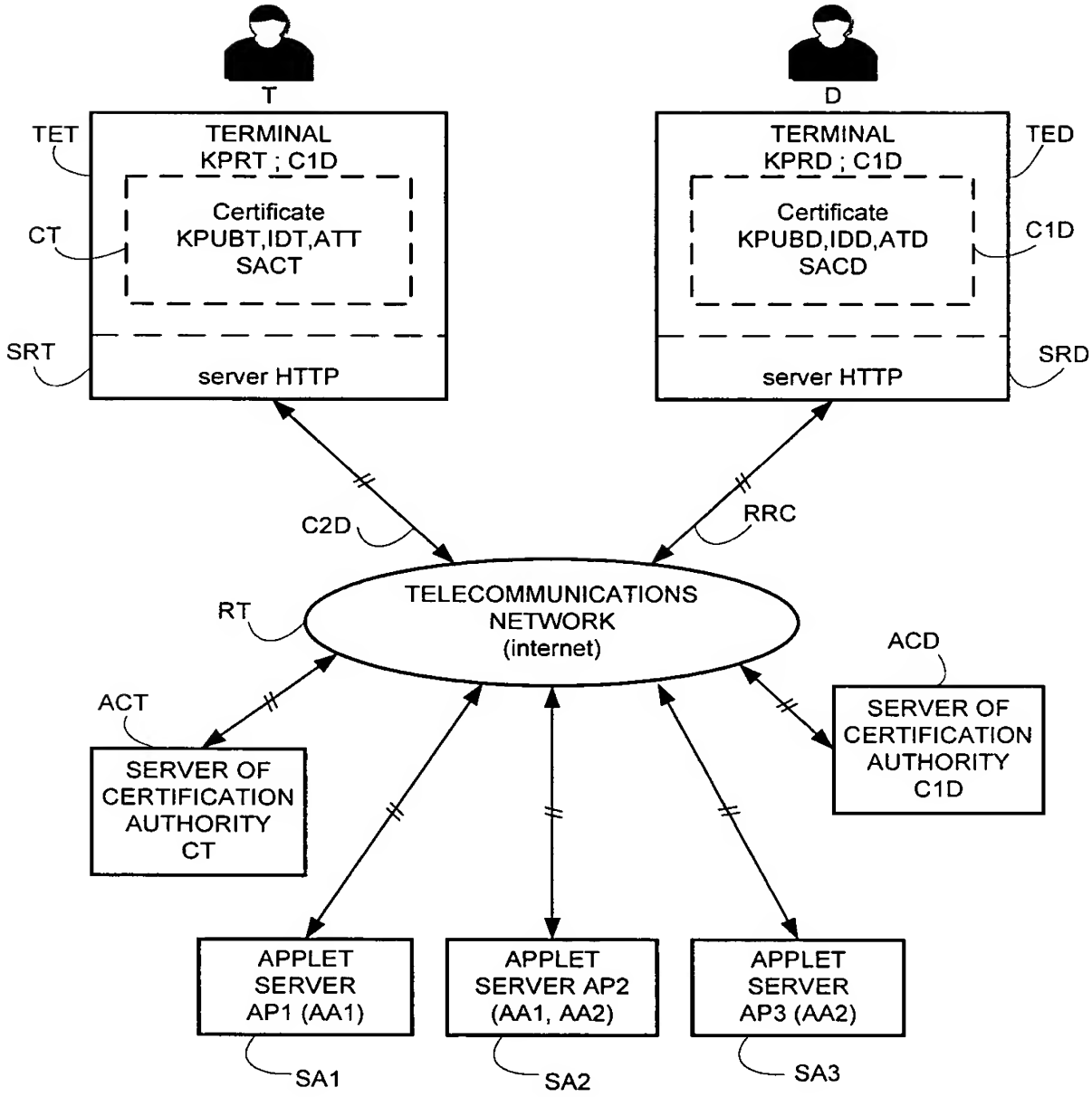
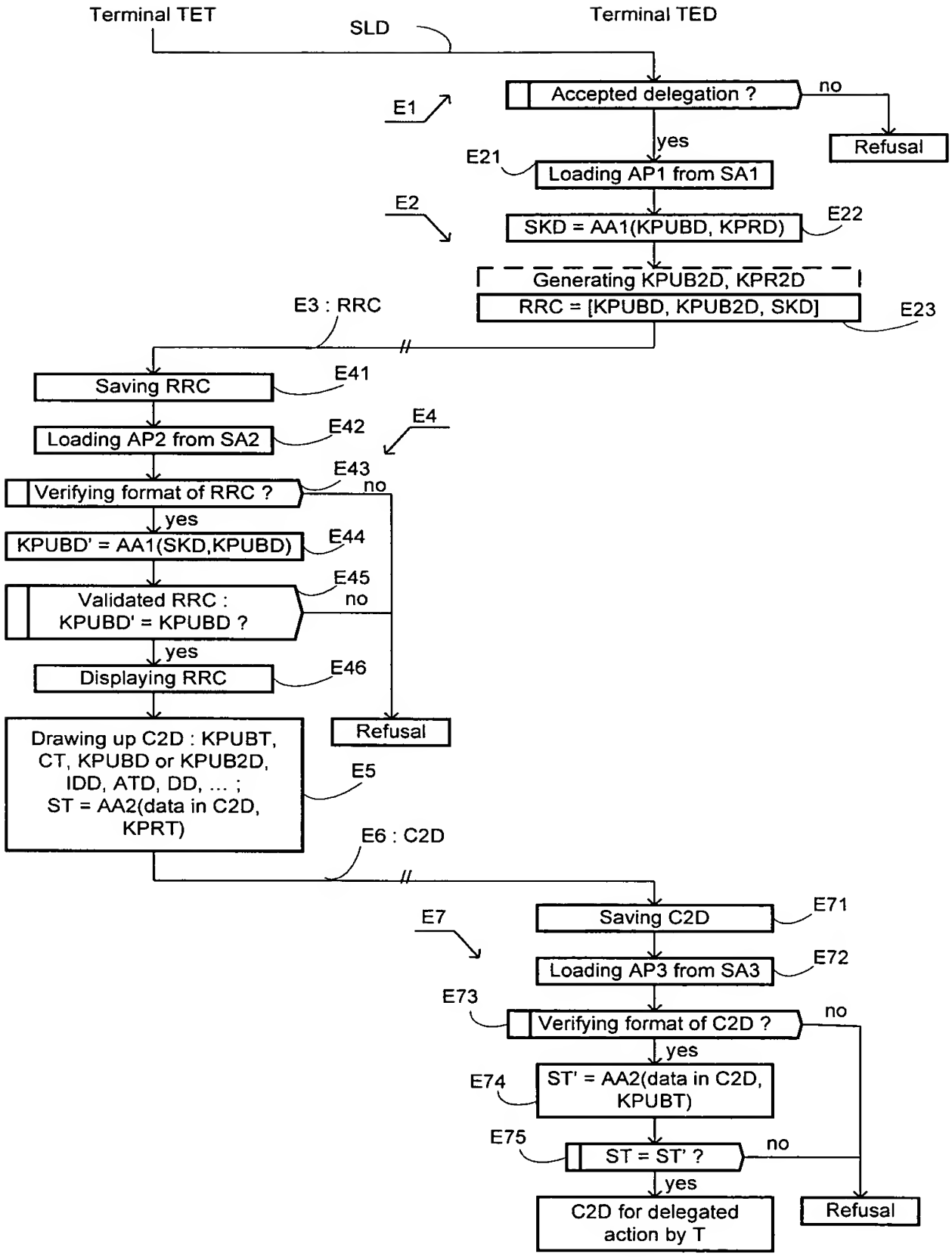

T
D
TET
TERMINAL
KPRT ; C1D
Certificate
KPUBT,IDT,ATT
SACT
CT
SRT
server HTTP
TERMINAL
KPRD ; C1D
Certificate
KPUBD,IDD,ATD
SACD
server HTTP
TED
C1D
SRD
C2D
RRC
RT
TELECOMMUNICATIONS
NETWORK
(internet)
ACD
ACT
SERVER OF
CERTIFICATION
AUTHORITY
CT
SERVER OF
CERTIFICATION
AUTHORITY
C1D
APPLET
SERVER
AP1 (AA1)
APPLET
SERVER AP2
(AA1, AA2)
APPLET
SERVER
AP3 (AA2)
SA1
SA2
SA3

FIG. 2


Terminal TET
SLD
Terminal TED
Accepted delegation ?
no
Refusal
E1
yes
E21
Loading AP1 from SA1
E2
SKD = AA1(KPUBD, KPRD)
E22
Generating KPUB2D, KPR2D
RRC = [KPUBD, KPUB2D, SKD]
E23
E3 : RRC
Saving RRC
E41
Loading AP2 from SA2
E42
E4
Verifying format of RRC ?
E43
no
yes
KPUBD' = AA1(SKD,KPUBD)
E44
Validated RRC : KPUBD' = KPUBD ?
E45
no
yes
Displaying RRC
E46
Refusal
Drawing up C2D : KPUBT, CT, KPUBD or KPUB2D, IDD, ATD, DD, ... ; ST = AA2(data in C2D, KPRT)
E5
E6 : C2D
E7
Saving C2D
E71
Loading AP3 from SA3
E72
E73
Verifying format of C2D ?
no
yes
E74
ST' = AA2(data in C2D, KPUBT)
E75
ST = ST' ?
no
yes
C2D for delegated action by T
Refusal